Frequently Ask Questions

1. What must I do to maintain the DMCC-S tablet?

The tablet must be connected at least once every 10 calendar days. The battery should be at least 25% charged before powering off. See EULA for details on device and accounts maintenance.

2. In what locations may I use the DMCC-S tablet?

The tablet will function where there is adequate cellular service; consult cellular provider online coverage maps. Consult your security and I.T. staff for other considerations. See EULA for details.

3. What should I do if I break the DMCC-S tablet or crack the screen?

Device manufacturer or third parties **may not** service the device. See EULA for details on replacing or repairing your device.

4. What peripherals are authorized for use with the DMCC-S tablet?

The **only** peripheral that may be used are **wired headphones** for voice calls. Other peripherals such as keyboards and pens are strictly prohibited. Charging the tablet with anything other than an A/C charger is also prohibited

5. Why is the Cellcrypt Auto-Start not available?

This feature is incompatible with the DMCC-S tablet. Auto-Register is an option that enables Cellcrypt to register to the call manager once the App has started.

Service Information

Capabilities

- Available to DoD Mission Partners
- Access to DoD Classified Email
- Secure phone calls to DMCC, Defense Red Switch Network (DRSN), Voice-Over Secure IP (VoSIP) and Secure Communications Interoperability Protocol (SCIP) devices
- Global Service Area utilizing commercial cellular (where available)
- Highly portable no (Classified) Data-at-Rest (DAR) solution
- Commercial Solutions for Classified (CSfC) standards based with competitively priced Tablet and Internet Service
- 24/7/365 Service Support

Service Support

DISA's DoD Enterprise Mobility Website
https://www.disa.mil/Enterprise-Services/Mobility/DOD-Mobility/DMCC/Secret

Need Immediate Assistance?

Contact the DMCC Service desk at DSN 312-850-0032 or Toll Free at 844-347-2457 (Option 4)

DISA

DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

DoD Mobility Classified Capability Secret (DMCC-S) Tablet

Quick Start Guide

www.disa.mil

Quick Start Instructions

Powering on the Device and Verifying VPN Connectivity

1. Power on the hotspot.
2. Power on the DMCC-S Tablet.
3. Once powered-on, enter the provided passcode
4. An illuminated white key symbol in the top status bar verifies VPN connectivity
   - **Note:** The DMCC-S device needs to remain within 25 feet of the Hotspot. The Hotspot requires a 3G, 4G or LTE signal with at least three signal bars for reliable service.
   - In some locations 3G may not provide adequate cellular service.
   - 2G service *will not* provide adequate data throughput.

How to Place or Receive Calls

1. Select the Cellcrypt application.
2. Insert *wired earphones* in headset jack.
3. Wait for the Cellcrypt top status bar icon to go from grey to green. This indicates you are ready to place or receive calls.
4. To Place a Call: Swipe 'Grey tab' upward to access dialing keypad or select a number from your contact list. Select the green phone icon to place your call.
5. To Receive a Call: When the device is ringing press the green phone icon to answer. (If earphones are not connected the call will drop).

To Access your Email

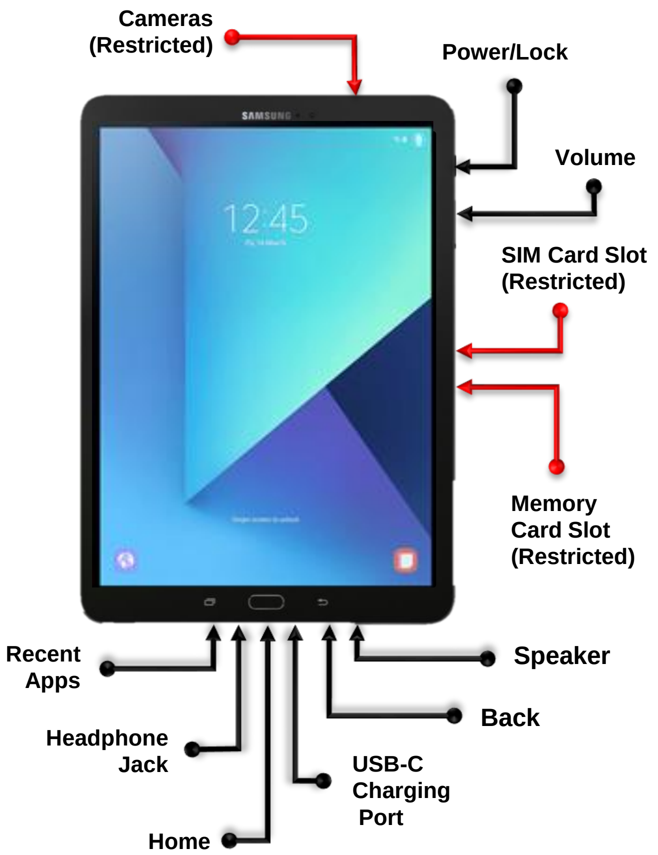
1. Open Chrome application
2. Enter in your Outlook Web Access URL in the browser (disregard if your URL is bookmarked)
3. When prompted select the certificate with your name and select 'Allow'.
4. After clicking "OK" on DoD Warning and Consent Banner you will be taken to your inbox.

Note: If you get a "Session Error" instead of your Inbox, click the link to open a new session.

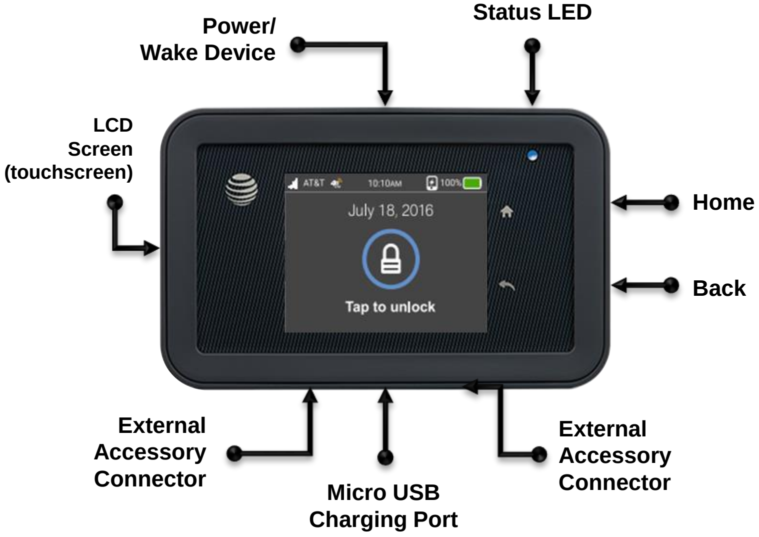
www.disa.mil

V3 28APR18

Device Overview



Hotspot Overview



Application Guide

Cellcrypt

This application is used to make secure calls after the VPN is active.

Chrome

This application permits access to secure web/data content. This app only allows access to Secure DoD Enterprise Email (DEE).

QuarkShield

This application is used to connect and confirm the secure VPN connection. *This connection must be active to use any of the features of the phone.*

Apps Icon

This presents all available applications on the device.

Switch Between Primary and Secondary VPN Connection

1. Open the QuarkShield Application.
2. Select the 3 dots to open the App Categories.
3. Select "VPN Category" (within the QuarkShield Application).
4. Select "Primary" or "Secondary" VPN. Select "Secondary" if the connection to the Primary VPN fails.
5. Select "Apply" and then close the application.

Note: Users may need to switch VPNs if an error occurs while connected to the VPN, the "key" symbol appears translucent, or is missing.